

# Oriented Steiner quasigroups

Izabella Stuhl

## Abstract

Motivated by applications in cryptography, we introduce the notion of an oriented Steiner quasigroup and develop elements of a related algebraic apparatus. The approach is based upon (modified) Schreier-type  $f$ -extensions for quasigroups (cf. earlier works [12, 9]) achieved through oriented Steiner triple systems. This is done in a fashion similar to in [11] where an analogous construction was established for loops. We briefly discuss an application of oriented Steiner triple systems in cryptography.

## 1 Introduction

A *Steiner triple system*  $\mathfrak{S}$  is an incidence structure consisting of points and blocks such that every two distinct points are contained in precisely one block and any block has precisely three points. A finite Steiner triple system with  $n$  points exists if and only if  $n \equiv 1$  or  $3 \pmod{6}$ .

A possible way to enrich Steiner triple systems is to introduce in each block a cyclic order. These objects occur in the literature as oriented Steiner triple systems  $(\mathfrak{S}, T)$  (see [14]) or as Mendelsohn triple systems (see [7] Section 28, p. 388).

Steiner triple systems play an important role in applications, particularly in cryptography, coding theory, statistics and computer science. Cf. [3], [5] (where a number of chapters are dedicated to this concept), and also [4] and the references therein. A particular example of an application is given in [13]. The results of the present paper develop an algebraic background that can be useful, e.g., in the context of [2].

A Steiner triple system  $\mathfrak{S}$  provides a multiplication on the set of pairs of different points  $x, y$  taking as product the third point of the block joining  $x$  and  $y$ . Defining  $x \cdot x = x$ , we get the Steiner quasigroup associated with  $\mathfrak{S}$ . Conversely, a Steiner quasigroup determines a Steiner triple system whose points are the elements of the quasigroup, and the blocks are the triples  $\{x, y, xy\}$  for  $x \neq y \in \mathfrak{S}$ .

---

2010 *Mathematics Subject Classification*: 20N05, 05B07, 94A60.

*Key words and phrases*: extensions of quasigroups, Steiner quasigroups, oriented Steiner triple systems, cryptography

Steiner triple systems and Steiner quasigroups are in a one-to-one correspondence, thus algebraic structures corresponding to the oriented systems are also of interest. We also note that a class of idempotent semi-symmetric quasigroups (also called Mendelsohn quasigroups) can be related to Mendelsohn triple systems (see e.g. Theorem 28.8 in [7] p. 389.)

In an earlier work [11] one studied loops corresponding to oriented Steiner triple systems obtained by a Schreier-type extension process (developed for loops in [8]). In this paper we determine classes of quasigroups related to oriented Steiner triple systems in the same way as it was done in [11]. Here we use modified Schreier-type  $f$ -extensions for quasigroups introduced in [12], [9]. Furthermore, we verify which properties are satisfied for these classes of quasigroups, among the properties discussed in [11] for the case of loops. Namely, we inspect alternative and flexible laws, inverse and cross inverse properties, Bol and Moufang identities. This provides some information about the similarity and diversity in the behavior of loops and quasigroups corresponding to the same oriented Steiner triple system.

In the final part of the paper we propose an encryption algorithm based on quasigroup extensions. In our view, this may open an application of oriented Steiner triple systems in cryptography, based on properties of oriented Steiner quasigroups.

## 2 Preliminaries

A quasigroup  $Q$  satisfies the *left inverse property* or the *right inverse property* if there exists a bijection  $\iota : Q \rightarrow Q$  such that the relation  $\iota(x) \cdot (x \cdot y) = y$  or  $(y \cdot x) \cdot \iota(x) = y$  holds for all  $x, y \in Q$ , respectively. If both the left and the right inverse properties hold in a quasigroup, then is said to have the *inverse property*. If for any  $x \in Q$  there exists an element  $x'$  such that  $(xy)x' = y$  for all  $y \in Q$  then  $Q$  has the *left cross inverse property* and if for any  $x \in Q$  there exists an element  $x''$  such that  $x''(yx) = y$  for all  $y \in Q$  then  $Q$  has the *right cross inverse property*. A quasigroup has the *cross inverse property* if satisfies both the left and the right cross inverse properties.  $Q$  is *left alternative*, respectively *right alternative* if  $x \cdot (x \cdot y) = x^2 \cdot y$ , respectively  $(y \cdot x) \cdot x = y \cdot x^2$  for all  $x, y \in Q$ . A quasigroup  $Q$  is *flexible* if  $x \cdot (y \cdot x) = (x \cdot y) \cdot x$  for all  $x, y \in Q$ . A quasigroup satisfying the identity  $x(yx) = y$  is called *semi-symmetric*.  $Q$  is a *left Bol quasigroup*, respectively *right Bol quasigroup* if it satisfies the identity  $x \cdot (y \cdot (x \cdot z)) = (x \cdot (y \cdot x)) \cdot z$ , respectively  $((x \cdot y) \cdot z) \cdot y = x \cdot ((y \cdot z) \cdot y)$ . A quasigroup that satisfies the left and the right Bol identity is a *Moufang quasigroup*. An idempotent totally symmetric quasigroup is called *Steiner quasigroup*. A totally symmetric loop of exponent 2 is called *Steiner loop*.

An *oriented Steiner loop*  $L$  is an extension of the group  $Z_2$  by a Steiner loop  $S$  for which there exists an oriented Steiner triple system  $(\mathfrak{S}, T)$  such

that the elements different from the identity of the Steiner loop  $S$  are the points of  $\mathfrak{S}$ , the restriction of the factor system of  $L$  to  $(\mathfrak{S} \times \mathfrak{S}) \setminus \{(x, x), x \in \mathfrak{S}\}$  coincides with the orientation function of  $(\mathfrak{S}, T)$  and  $f(x, x) = -1$ , respectively  $f(x, x) = 1$  for all  $x \in S \setminus \{e\}$  holds. Cf. Definition 4 in [11], p. 136.

Oriented Steiner loops related to oriented Steiner triple systems, in such a way that two non-isomorphic loops are related to the same oriented Steiner triple system. In a similar manner we deal with oriented Steiner quasigroups; to associate a unique quasigroup to an oriented Steiner triple system we also consider extensions of an object of order 3.

Let  $Q, K$  be quasigroups and let  $f$  be a function  $f : Q \times Q \rightarrow K$ . Consider the operation

$$(a, \alpha) \circ (b, \beta) := (ab, f(a, b) \cdot \alpha\beta),$$

defined on the set  $Q \times K = \{(a, \alpha), a \in Q, \alpha \in K\}$ . Since the equations  $(a, \alpha) \circ (x, \xi) = (b, \beta)$  and  $(x, \xi) \circ (a, \alpha) = (b, \beta)$  have unique solutions  $\mathcal{Q}_f = (Q \times K, \circ)$  is a quasigroup. Moreover, the mapping  $(Q \times K, \circ) \rightarrow Q : (a, \alpha) \mapsto a$  is a quasigroup homomorphism. The quasigroup  $\mathcal{Q}_f$  is an *f-extension of the quasigroup  $K$  by the quasigroup  $Q$* . The map  $\varphi_f : \mathcal{Q}_f \rightarrow Q : (a, \alpha) \mapsto a$  is the related homomorphism of the *f-extension  $\mathcal{Q}_f$* . The kernel of  $\varphi_f$  is a quasigroup congruence; its classes are the equivalence classes of the *f-extension*.

### 3 Extensions of commutative quasigroups of order three

**Theorem 1** *Let  $(Q, \cdot)$  and  $(K, +)$  be two quasigroups. Suppose  $(K, *)$  is a quasigroup isotopic to  $(K, +)$  via a principal isotopism  $(\alpha + \beta) = \varphi_1(\alpha) * \varphi_2(\beta)$ . Let the map  $T = (id, \tau)$  be defined by  $(a, \alpha) \mapsto (a, \tau(\alpha))$ , where  $\tau$  is an automorphism of  $K$ .*

- (i) *If  $\varphi_1 = \varphi_2 = \tau$  is an involutory automorphism, then the quasigroup extensions  $\mathcal{Q}_f^+ := (Q \times K, +, f)$  and  $\mathcal{Q}_f^* := (Q \times K, *, g)$  are isomorphic if and only if  $f(a, b) = g(a, b)$  for all  $a, b \in Q$ .*
- (ii) *For involutory automorphisms  $\varphi_1 = \varphi_2, \tau$  the quasigroup extensions  $\mathcal{Q}_f^+ := (Q \times K, +, f)$  and  $\mathcal{Q}_g^* := (Q \times K, *, g)$  are isomorphic if and only if  $\varphi_2(\tau(f(a, b))) = g(a, b)$  for all  $a, b \in Q$ .*

**Proof.** For the map  $T = (id, \tau) : \mathcal{Q}_f^+ \rightarrow \mathcal{Q}_g^*$  we have

$$\begin{aligned} T((a, \alpha) + (b, \beta)) &= T(ab, (\alpha + \beta) + f(a, b)) \\ &= (ab, \tau((\alpha + \beta) + f(a, b))) = (ab, (\tau(\alpha) + \tau(\beta)) + \tau(f(a, b))) \\ &= (ab, \varphi_1(\varphi_1(\tau(\alpha)) * \varphi_2(\tau(\beta))) * \varphi_2(\tau(f(a, b)))) \end{aligned}$$

with  $\varphi_1 = \varphi_2$  equal to  $(ab, (\tau(\alpha) * \tau(\beta)) * \varphi_2(\tau(f(a, b))))$  and with

$$\varphi_2(\tau(f(a, b))) = g(a, b), \quad (ab, (\tau(\alpha) * \tau(\beta)) * g(a, b)) = T(a, \alpha) * T(b, \beta)$$

for all  $a, b \in Q$ .

If, in addition  $\varphi_1 = \varphi_2 = \tau$  then  $g(a, b) = \varphi_2(\tau(f(a, b))) = f(a, b)$ .  $\blacksquare$

There are three commutative quasigroups of order 3, one of which is the cyclic group  $Z_3$  of order 3. The second one is a commutative quasigroup that has an idempotent element. But then all three elements are idempotent, and we get the Steiner quasigroup  $K_3$  of order 3. The third quasigroup  $Q_3$  is a commutative quasigroup that has no idempotent element. The group  $Z_3 = (\{\alpha, \beta, \gamma = e\}, +)$  is a principal isotope of  $K_3 = (\{\alpha, \beta, \gamma\}, *)$  and of  $Q_3 = (\{\alpha, \beta, \gamma\}, \diamond)$ , with  $\alpha * \beta = \varphi_1(\alpha) + \varphi_2(\beta) = -\alpha - \beta$  and  $\alpha \diamond \beta = \varphi_1(\alpha) + \varphi_2(\beta) = -\alpha - \beta - e$ , respectively.

Theorem 1 implies

**Corollary 2** *Quasigroup  $f$ -extensions of  $Z_3$  by  $Q$ ,  $K_3$  by  $Q$  and  $Q_3$  by  $Q$  with the same factor system are isomorphic for any quasigroup  $Q$ .*

**Proof.** The claim for the first and the second extensions is obtained by choosing equal involutory automorphisms  $\varphi_1 = \varphi_2 = \tau$  given by  $\alpha \mapsto -\alpha$  for all  $\alpha$ . In the case of the first and the third extensions the map  $T = (id, \tau) : (Q \times Q_3, \diamond, g) \longrightarrow (Q \times Z_3, +, f)$  is an isomorphism with  $\tau : \alpha \in Q_3 \mapsto -\alpha \in Z_3$ .  $\blacksquare$

## 4 Quasigroups corresponding to oriented Steiner triple systems

With any oriented Steiner triple system  $(\mathfrak{S}, T)$  one can associate a function  $f^* : \mathfrak{S} \times \mathfrak{S} \setminus \{(x, x); x \in \mathfrak{S}\} \longrightarrow \{\pm 1\}$  called the *orientation function* of  $(\mathfrak{S}, T)$ . If  $a_1, a_2$  are distinct points determining the oriented block  $(a_1, a_2, a_3)$ , then  $f^*(a_1, a_2) = 1$  and  $f^*(a_2, a_1) = -1$ .

Using orientation functions, we determine the factor system of the  $f$ -extensions which yield the corresponding quasigroups.

As Steiner quasigroups are commutative inverse property quasigroups, Steiner quasigroups satisfying left or right Bol identity are Moufang. According to [6], quasigroups fulfilling any one of the Moufang identities have a unit element. Steiner quasigroups do not possess the alternative law:  $y = (yx)x \neq y \cdot x^2 = yx$ . These facts imply that quasigroups related to oriented Steiner triple systems via  $f$ -extensions by Steiner quasigroups

associated with the non oriented Steiner triple systems cannot be Bol or Moufang quasigroups and cannot have the alternative law.

Furthermore, the left, middle and right nuclear square conditions

$$(xx)(yz) = ((xx)y)z, \quad x((yy)z) = (x(yy))z, \quad x(y(zz)) = (xy)(zz)$$

in Steiner quasigroups yield the associativity law because of idempotency. But the associative Steiner quasigroup must be the trivial of order 1. Thus, the quasigroups obtained as the above  $f$ -extensions cannot be left, middle or right nuclear square.

#### 4.1 Oriented Steiner quasigroups

Similarly to Definition 4 in [11], p. 136, we propose

**Definition 3** *An oriented Steiner quasigroup  $\mathcal{Q}_f^+$  ( $\mathcal{Q}_f^-$ ) is an  $f$ -extension of the cyclic group  $Z_2$  of order 2 by the Steiner quasigroup  $Q$  for which there exists an oriented Steiner triple system  $(\mathfrak{S}, T)$  with the following properties. (i) The elements of the Steiner quasigroup  $Q$  are the points of  $\mathfrak{S}$ . (ii) The restriction of the factor system of  $\mathcal{Q}_f^+$  ( $\mathcal{Q}_f^-$ ) to  $(\mathfrak{S} \times \mathfrak{S}) \setminus \{(x, x), x \in \mathfrak{S}\}$  coincides with the orientation function of  $(\mathfrak{S}, T)$ . (iii)  $f(x, x) = 1$ , (respectively  $f(x, x) = -1$ ) for all  $x \in Q$ .*

**Theorem 4** *Oriented Steiner quasigroups are flexible and have the cross inverse property.*

**Proof.** The statements follow from Remark 1 [11] p. 134. and Proposition 3.10 [8] p. 767. The bijection  $\kappa$  that determines the left and the right cross inverse property has  $\kappa : (a, \alpha) \mapsto (a, \alpha)$  for any  $a \in Q$  and  $\alpha \in Z_2$ . ■

Since each element is its own cross inverse element, we obtain

**Corollary 5** *Oriented Steiner quasigroups are semi-symmetric.*

We note that the obtained classes of quasigroups differ from the class of Mendelsohn quasigroups, since they are not idempotent. We have that  $(a, -1)(a, -1) = (a, 1)$  in  $\mathcal{Q}_f^+$  and  $(a, 1)(a, 1) = (a, -1)$  in  $\mathcal{Q}_f^-$  for all  $a \in Q$ .

The oriented Steiner quasigroups do not satisfy the left (right) alternative law (see Section 4) or the left (right) inverse property. (The latter means that  $\iota(a, \alpha)[(a, \alpha)(b, \beta)] = (b, \beta)$  with  $\iota(a, \alpha) = (a, -\alpha)$  which does not hold for  $a = b$  and  $\alpha = \beta$ .) This shows a difference with the case for oriented Steiner loops of exponent 4. However, the oriented Steiner quasigroups are flexible and have the cross inverse property, like oriented Steiner loops of exponent 2 (see Theorem 5, [11], p. 136.).

## 4.2 Canonical oriented Steiner quasigroups

We now turn back to the  $f$ -extensions of commutative quasigroups of order 3. We saw in Section 3 that in order to get a unique algebraic face of an oriented Steiner triple system as quasigroup  $f$ -extensions of the Steiner quasigroup of order 3 by Steiner quasigroups, we can restrict our consideration to the case of the  $f$ -extensions of the group of order 3 by Steiner quasigroups.

**Definition 6** *A canonical oriented Steiner quasigroup  $\mathcal{Q}_f$  is an  $f$ -extension of the cyclic group  $Z_3$  of order 3 by the Steiner quasigroup  $Q$  for which there exists an oriented Steiner triple system  $(\mathfrak{S}, T)$  with the following properties. (i) The elements of the Steiner quasigroup  $Q$  are the points of  $\mathfrak{S}$ . (ii) The restriction of the factor system of  $\mathcal{Q}_f$  to  $(\mathfrak{S} \times \mathfrak{S}) \setminus \{(x, x), x \in \mathfrak{S}\}$  coincides with the orientation function of  $(\mathfrak{S}, T)$ . (iii)  $f(x, x) = 0$  for all  $x \in Q$ .*

**Theorem 7** *The canonical oriented Steiner quasigroups satisfy the inverse property.*

**Proof.**  $Q$  is commutative, has the inverse property and the bijection  $\iota : \mathcal{Q}_f \rightarrow \mathcal{Q}_f : (a, \alpha) \mapsto (a, -\alpha)$  for all  $a \in Q$  and  $\alpha \in Z_3$  yields the right and the left inverse property of  $\mathcal{Q}_f$ . ■

The canonical oriented Steiner quasigroups are not flexible. This is deduced, with the help of Proposition 3.10 in [8] p. 767, from the fact that

$$f(x, yx)f(y, x) \neq f(xy, x)f(x, y) \text{ for all } x, y \in Q.$$

Next, the canonical oriented Steiner quasigroups are not idempotent. This follows from the fact that

$$(a, \alpha)(a, \alpha) = (a, \alpha + \alpha) = (a, -\alpha) \text{ for all } a \in Q, \alpha \in Z_3.$$

Further, the canonical oriented Steiner quasigroups do not have the cross inverse property:

$$[(a, \alpha)(b, \beta)](x, \delta(a, \alpha)) = (b, \beta) \text{ with } x = a \text{ and } \delta(a, \alpha) = (1 - \alpha),$$

and

$$(y, \xi(a, \alpha))[(b, \beta)(a, \alpha)] = (b, \beta) \text{ with } y = a \text{ and } \xi(a, \alpha) = (-1 - \alpha).$$

In fact, both of them fail to hold in the case  $a = b, \alpha = \beta$ .

Finally, the canonical oriented Steiner quasigroups are not semi-symmetric:

$$(a, \alpha)[(b, \beta)(a, \alpha)] = (b, 1 + \alpha + \alpha + \beta) \neq (b, \beta).$$

## 5 Near-associativity

Canonical oriented and oriented Steiner quasigroups are not loops. Hence, to measure their near-associativity we can consider the Belousov's generalization of the notion of nuclei (the orbits of the groups of regular permutations of the quasigroup). Cf. [1] p. 22–25.

A bijection  $\lambda : Q \rightarrow Q$  is a *left-regular permutation* or a *right-regular permutation* of  $(Q, \cdot)$ , if for all  $x, y \in Q$  one has  $\lambda(xy) = \lambda(x) \cdot y$  or  $\rho(xy) = x \cdot \rho(y)$ , respectively. If  $\lambda$  is a left-regular permutation then  $\lambda = \lambda_{\lambda(x)}\lambda_x^{-1}$  for all  $x \in Q$ . Similarly, if  $\rho$  is a right-regular permutation then  $\rho = \rho_{\rho(x)}\rho_x^{-1}$  for all  $x \in Q$ . Hence the left-regular permutations form a subgroup  $\Lambda(Q)$  of the left multiplication group  $G_l(Q)$ , and the right-regular permutations form a subgroup  $R(Q)$  of the right multiplication group  $G_r(Q)$ . If  $\Lambda(Q)$  or  $R(Q)$  consists only of the identity map of  $Q$ , then we say that the group of left-regular permutations or the group of right-regular permutations is *trivial*.

Steiner quasigroups are idempotent; consequently, they have only trivial right regular permutations. According to Remark 3.1 in [12], p. 113., the orbits of the group of right regular permutations of Steiner quasigroups are contained in the congruence classes of the  $f$ -extensions. Since we extend by idempotent quasigroups, these equivalence classes are normal sub-quasigroups of (canonical) oriented Steiner quasigroups.

**Proposition 8** *The group of the right regular permutations and the group of the left regular permutations, of an oriented Steiner quasigroup, are both isomorphic to the group  $Z_2$ . The group of right regular permutations and the group of left regular permutations, of a canonical oriented Steiner quasigroup, are both isomorphic to the group  $Z_3$ .*

**Proof.** The claims are deduced from Theorem 3.1 and Theorem 4.2 in [12], p. 113. and p. 115. ■

**Remark 9** *In the spirit of this generalization of the nucleus, (canonical) oriented Steiner quasigroups are right nuclear  $f$ -extensions. This is true because the orbits of the group of right regular permutations of the oriented Steiner quasigroup  $R(Q_f^+)$  ( $R(Q_f^-)$ ) and of the canonical oriented Steiner quasigroup  $R(Q_f)$  coincide with the congruence classes of the  $f$ -extensions  $\{(a, \alpha) : \alpha \in Z_2\}$  and  $\{(a, \alpha) : \alpha \in Z_3\}$ , respectively.*

*Also, (canonical) oriented Steiner quasigroups are left nuclear extensions, because the same argument is valid for the orbits of the group of left regular permutations.*

*Thus, (canonical) oriented Steiner quasigroups are nuclear  $f$ -extensions.*

## 6 Oriented Steiner triple systems in cryptology

It is commonly recognized that cryptology consists of two parts: *cryptography* - used for "defence", i.e., for constructing ciphers, - and *cryptanalysis* - used for "attacks", i.e., for developing methods on breaking ciphers. (The latter is often treated as a kind of an "art" based on case-by-case actions.) A cipher is a device, or a method, of information encryption, used with a purpose of enhancing security. A *private key* is a "hidden" collection of parameters of a cipher made known to the recipient but not divulged to the public. A number of constructions of error detecting and error correcting codes, cryptographic algorithms and enciphering systems have been constructed with the help of some associative algebraic structures. However, there exists also a possibility of using non-associative structures such as quasigroups and neo-fields. Sometimes codes and ciphers based on non-associative structures display better qualities than codes and ciphers based on associative structures. On the other hand, efficiency of applications of quasigroups in both cryptography and cryptanalysis is based on the fact that quasigroups can be interpreted as "generalized permutations". (The number of quasigroups of order  $n$  exceeds  $n! \cdot (n-1)! \cdot \dots \cdot 2! \cdot 1!$ .) The ratio of the number of groups to the number of quasigroups of a given size tends to zero as the size tends to infinity. A survey of results about quasigroups in cryptology can be found in [10] and in the references therein.

Now, we propose an encryption algorithm based on quasigroups using their extensions. Let  $K$ ,  $Q$  be arbitrary quasigroups, and consider the Schreier-type quasigroup extension  $\mathcal{Q}$  defined on  $Q \times K$  by the operation:

$$(a, \alpha) \circ (b, \beta) = (ab, f(a, b)\alpha^{G(b)}\beta),$$

where  $f : Q \times Q \longrightarrow K$ , and  $G : Q \longrightarrow \text{Aut}(K)$ .

The message is a string  $q = (q_1, q_2, \dots, q_n)$  consisting of elements of  $Q$ . The public key is formed by strings  $k = (k_1, k_2, \dots, k_n)$ , ( $k_i \in K$ ) and  $c = (c_1, \dots, c_n)$ ,  $c_i \in \mathcal{Q}$ . The private key consists of function  $f$  and automorphism  $G$ . The enciphered message is a string  $a = (a_1 = (q_1, k_1) \circ c_1, a_2 = (q_2, k_2) \circ c_2, \dots, a_n = (q_n, k_n) \circ c_n)$  consisting of elements of  $\mathcal{Q}$ . The sender broadcasts both the ciphertext  $a$  and the keys  $k$ , and  $c$ .

Quasigroup  $\mathcal{Q}$  (i.e., its multiplication table) is also distributed as a public part of the key. The security lies in the function  $f$  and in the map  $G$ . For sufficiently large quasigroups the cryptanalyst will face a difficult task to decode the ciphertext without knowing  $f$  and  $G$ . In fact, a possible interceptor may have  $a$ ,  $k$  and  $c$ , but must find out the original message  $q$ ; and even possible successes with deciphering past messages may not help in future in the case of large quasigroups  $K, Q$ .

The intended receiver of course knows  $f$ , and  $G$ , gets  $a$ ,  $k$ ,  $c$ .



As an example, we apply a simplified version of this algorithm, to show how oriented Steiner triple systems can occur in enciphering, using canonical oriented Steiner quasigroups.

As before, let  $(\mathfrak{S}, T)$  be an oriented Steiner triple system,  $Q$  be a Steiner quasigroup formed by points of  $(\mathfrak{S}, T)$ . Then  $\mathcal{Q}_f$  is the associated canonical oriented Steiner quasigroup (i.e., the  $f$ -extension of  $Z_3$  by  $Q$  with the factor system  $f$ , determined by the orientation function of the oriented Steiner triple system  $(\mathfrak{S}, T)$ ).

A message  $q$  is given as a sequence  $q_1, \dots, q_n$  of points of the oriented Steiner triple system, (elements of the quasigroup  $Q$ ), and public keys are sequences  $k_1, \dots, k_n \in Z_3$  and  $c_1, \dots, c_n \in \mathcal{Q}_f$ . The ciphertext is  $a_1 = (q_1, k_1) \circ c_1, \dots, a_n = (q_n, k_n) \circ c_n$ .

The sender transmits the enciphered message and keys. Orientations of blocks are known only by the intended receiver.

The effectiveness of this algorithm is related to the fact that the blocks of the Steiner triple system are oriented independently. Thus, from a Steiner triple systems with  $n$  points and  $b = \frac{n(n-1)}{6}$  blocks one can construct  $2^b$  oriented Steiner triple systems.

The same algorithm is working in the case of oriented Steiner quasigroups.

### Acknowledgement

The author has been supported by FAPESP Grant - process No 11/51845-5, and expresses her gratitude to IMS, University of São Paulo, Brazil, for the warm hospitality.

### References

- [1] V. D. Belousov, Foundations of the theory of quasigroups and loops, (Russian). *Nauka, Moscow (1967)*.
- [2] F. E. Bennett, Quasigroups. In: C.J. Colbourn, J.H. Dinitz (Eds.), Handbook of Combinatorial Designs, 2nd edition, *Chapman and Hall/CRC Press, (2007) 424429*.
- [3] C. J. Colbourn, J.H. Dinitz (Eds.), Handbook of Combinatorial Designs, 2nd edition. *Chapman and Hall/CRC Press, 2007*.
- [4] C. J. Colbourn, A. Rosa, Triple systems. *Oxford University Press, New York, 1999*.
- [5] J. H. Dinitz, D.R. Stinson, Contemporary design theory: A collection of surveys. *Wiley, New York, 1992*.
- [6] K. Kunen, Moufang quasigroups. *J. Algebra, 183, (1996) 231-234*.

- [7] E. Mendelsohn, Mendelsohn designs. In: C.J. Colbourn, J.H. Dinitz (Eds.), Handbook of Combinatorial Designs, 2nd edition, *Chapman and Hall/CRC Press*, (2007) 388393.
- [8] P. T. Nagy, K. Strambach, Schreier loops. *Czechoslovak Math. J.*, 58 (133), (2008) 759-786.
- [9] P. T. Nagy, I. Stuhl, Right nuclei of quasigroup extensions. *Comm. in Alg.*, 40, (2012) 1893-1900.
- [10] V. A. Shcherbacov, Quasigroups in cryptology, *Comp. Sci. J. Moldova*, 17, (50), (2009) 193-228.
- [11] K. Strambach, I. Stuhl, Oriented Steiner loops. *Beiträge zur Algebra und Geometrie*, 54, (2013) 131-145.
- [12] I. Stuhl, Regular permutations of quasigroups. *J. of Adv. Math. Studies*, 3, (2010) 111-116.
- [13] B. Vasic, Structured iteratively decodable codes based on Steiner systems and their application in magnetic recording. *Global Telecommunications Conference*, 5, (2001), 2954-2960.
- [14] S. Walter, Geordnete Steinersche Tripelsysteme. *Dissertation, Universität Erlangen-Nürnberg* (1983).

Izabella Stuhl  
 Institute of Mathematics and Statistics  
 University of São Paulo  
 05508-090 São Paulo, SP, Brazil  
 University of Debrecen  
 H-4010 Debrecen, Hungary  
*E-mail:* izabella@ime.usp.br